编制编写政务系统网络安全风险评估报告

产品名称	编制编写政务系统网络安全风险评估报告
公司名称	河南世耀诚实业集团有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:文案定制 服务方向:专业领域
公司地址	南阳市卧龙区工业路华龙广告二楼
联系电话	13140513661 18338218580

产品详情

“ 互联网+ ”给人们的生活带来了极大的便利，面对高速发展的互联网，人们对其的认同度在日益增加。但是，互联开放的网络，资源交流便捷的同时，信息泄漏的隐患在逐渐加剧。

尤其是与民生息息相关的政务部门。要知道，政务系统信息网络的安全与否，直接对政务信息资产的安全产生着重要的影响。

因而，重视政务系统的信息网络安全及其防护人员，对政务系统信息网络安全进行风险评估，能有效的预防和解决潜在的信息安全威胁，进一步对政务系统信息网络安全进行保障，促进政务网络建设的健康发展。

那么，何为信息网络安全风险评估？为政务系统做信息安全风险评估的意义何在？电子政务系统面临哪些安全风险？如何做好政务系统的信息安全风险评估工作？

何为信息安全风险评估？就是以风险管理角度，利用全面有效的科学方法和手段，对系统及网络所面临的一切威胁和隐患，进行系统、完整的分析与评估，保证整个信息网络能够安全、平稳的运行下去。

信息安全风险评估有两种形式，一是自评估，二是检查评估。

自评估：是指电脑系统自带的、运营中的、或者单位自行发起的风险评估；

检查评估：是指国家及系统管理部门遵循法律法规对网络安全实施的风险评估。

通常，信息安全风险评估是以自评估为主，而自评估与检查评估相辅相成，遵循严密组织、规范操作、科学有效的原则。

自评估和检查评估可以以自身技术力量为寄托，也可以向第三方机构寻求技术帮助。

信息安全风险评估的工作原理是对系统所采用的安全策略和管理制度进行评估审核。

针对不合理之处，有效采取措施，检查可能存在的漏洞；

针对评估的风险指数，采取不同的针对措施；

根据检查制定出系统化的检查报告，方便系统管理人弥补漏洞。

如此，才能为为网络安全做进一步保障依据，提高整体的网络安全水平。

政务系统信息安全风险评估的意义何在？

政务作为国家组织的重要组成结构，对国家的发展具有导向作用，政务系统信息存储着大量的有效信息，关乎着人民的切身利益，一旦发生信息泄漏，对人民及国家安全性会造成一定程度的威胁。

基于此，保证政务系统的正常运作，对政务系统进行安全风险评估，是非常必要且应给予高度重视的。

对政务系统做信息网络安全风险评估，是建设政务信息安全的根基。利用信息技术的高效便捷，进行政务信息的收集以及管理，从而减少相关业务人员的工作压力，大大提高工作的时效性。同时，还能为整个信息安全建设打好基础，

政务信息网络安全风险评估是信息安全管理的“利器”，它能够及时发现政务网络系统可能出现的的信息安全漏洞，对现状下的网络信息系统进行安全性能评估，为信息安全管理提出危险警示，利用模拟化系统攻击的方式对可能出现的安全漏洞进行摸索排查，将网络信息系统危险降到比较低，对政务网络安全系统的管理提供强有力的保障。

信息系统风险评估主要是针对系统可能出现的安全隐患进行分析，消除掉这些安全隐患，切实保障政务网络信息系统的高效运行。信息系统风险评估花费成本较低，且能起到良好的信息系统安全预防作用，是寻求适度安全和建设成本的良佳点。

在进行网络信息系统安全检测时，既要借鉴先进经验，取其精华弃其糟粕，学习优秀网络信息安全管理措施，又要重视预警防范，加大网络信息安全风险评估的开展，减少网络安全隐患的存在，为政务网络信息系统建立安全良好的网络环境。

电子政务系统所面临的安全风险

1、非法入侵黑客组织：互联网的高速发展带来的巨大经济利益，时刻吸引着网络上拿的不法的黑客组织。在金钱与权力的诱惑下，非法入侵电子政务网络信息系统，窃取相关数据资料，为政务以及国家带来严重资源损失，甚至威胁到广大群众的个人安全以及切身利益。

2、计算机病毒威胁：计算机是由大量芯片软件组装而成的精密的电子设备，是网络信息系统建立的主要实施对象。而如今的计算机，功能越来越强大，软件开发应用更加丰富，数据计算更加精
准，AI智能模拟操作直观便捷。

但同时，也产生了很多计算机病毒。它们乘虚而入，攻击网络信息系统，扰乱资料信息的编排，丢失相关资料文献等，对网络信息系统的安全造成了一定的威胁。

3、内网系统本身漏洞：政务网络信息系统自身出现的漏洞，亦会导致整个网络系统造成瘫痪，导致重要数据丢失，为政务机构带来损失。因此，政务信息网络系统建立过程中一定要严格把控每一
流程步骤，环环相扣。

同时，进行模拟入侵实验，不断修改强化应用程序，而后在完成内网系统建立后，一定要多次重复进行预试验，减少实验差错，及时纠正系统错误，避免出现系统自身漏洞，给计算机病毒以及非法入侵黑客组织留下可乘之机。

4、内部人员泄密：内部人员是政务系统信息网络安全的重大“ 缺口 ”，在相关政务机构在进行业务人员选拔时，一定要综合多方面因素，选择比较适合网络信息安全方面的人才。

同时对业务人员要定期举行信息安全教育培训，强化自身职业操守，提升个人思想道德建设，不断丰富自身知识储备，提升网络信息系统安全意识，加强内部人员的规范化管理，避免内部人员泄密的事件循环发生。

5、用户安全意识淡薄：这是一个普遍的现象。大多数的人会认为：政务系统怎么会出现问题？基于安全意识淡薄，网络知识匮乏，进而导致政务网络系统服务器出现故障，整个系统处于瘫痪状态，无法保障正常运作，对政务工作高效开展造成了一定程度影响。

6、系统安全软件本身的威胁：要知道，系统安全软件本身，有时候也会对电子政务系统进行攻击，造成系统损伤，无法正常进行运转。这就需要专 业安全人员的明确分辨了，在不断提升自身技术水平，探索不同情境下政务系统面临的攻击，把握特点，逐一击破，保证政务系统的安全运作。

做好电子政务系统安全风险评估

明确职责与工作机制，提升应急处置能力，合力提高国家网络安全保障水平。

电子政务面临的主要威胁来自高 级黑客或者有组织的网络犯罪集团以及敌对国家机构和组织，各机构现

有的技术力量普遍难以应对上述威胁。

建议在继续做好基本安全加固工作的基础上，对现有国家 级信息安全力量进行梳理：

统筹规划和发展，明确各机构职责和各机构之间的协调合作机制，加强技术力量建设。

在安全态势感知、威胁监测、漏洞分析等环节上下细功夫，加强威胁和漏洞预警及信息共享。

加强对重要网络安全域和业务系统的全面信息安全风险评估，识别安全隐患，并评估对重要信息系统的影响。

完善应急预案，建立综合应急指挥平台和体系，加强突发事件应急演练，增加应急人员能力培训，提升综合应急处置能力。

建设国家 级网络安全防护体系，形成强大的国家网络安全保障能力，集中优势资源保障国家重要信息系统安全稳定。

加强电子政务信息系统安全风险管理技术。适应社会发展的进程，完善电子政务信息系统安全风险管理机制。

安全风险评估是信息安全防护的重点手段之一，完善电子政务信息系统的安全风险管理机制，才能知道，信息系统的不安全因素是什么，该采取什么样的措施解决这些不安全因素。

同时，建立完善的信息系统安全评估风险管理机制，也是信息管理部门的重点工作，可以方便安全人员们做好后期记录与审查工作，及时了解故障出现的原因，帮助政务系统进一步完善安全管理体系。